ASA有高CPU使用情况由于流量环路，当VPN客户端断开

目录

简介

本文描述发生的常见问题，当从该思科可适应的安全工具(ASA)的VPN客户端断开运行作为远程访问VPN头端。本文也描述流量环路出现，当VPN从ASA防火墙的用户断开的情况。本文不包括如何配置或从某些普通的路由配置出现对VPN的设置远程访问，只有特殊的例子。

先决条件

要求

Cisco 建议您了解以下主题：

- 在ASA的远程访问VPN配置
- 基本层3路由的概念

使用的组件

本文档中的信息根据运行ASA代码版本9.1(1)的ASA型号5520。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

相关产品

本文可以与这些硬件和软件版本一起使用：

- 任何ASA型号
- 任何ASA代码版本

背景信息

当用户连接对ASA作为远程访问虚拟专用网集中器时， ASA在ASA路由表里安装一个招待基础的路由该路由流量给该VPN客户端在外部接口外面(往互联网)。当该用户断开时，路由从表删除，并且在网络内部的数据包(被注定对那断开VPN用户)也许循环在ASA和一个内部路由设备之间。

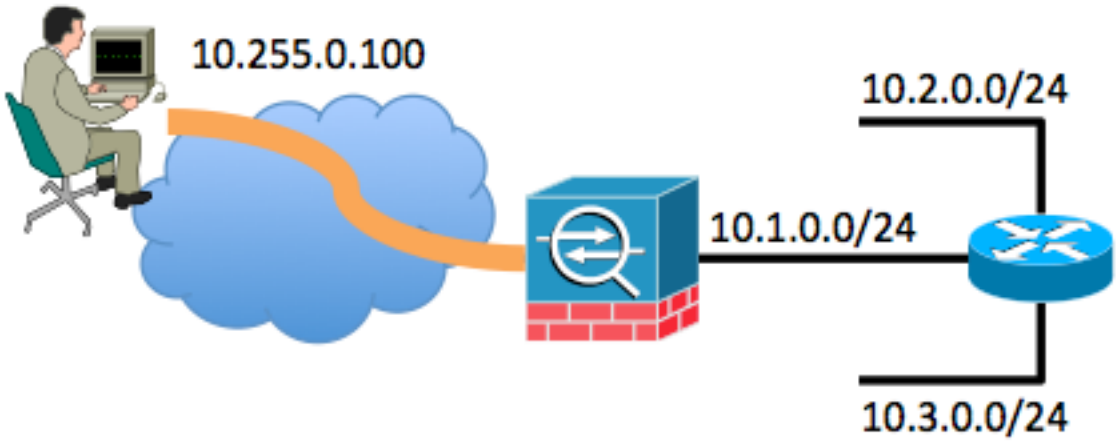
另一问题是被导向的(网络)广播包(生成由VPN客户端的删除)也许由ASA转发作为往内部网络的单播帧。这也许转发它回到ASA，造成数据包循环，直到存活时间(TTL)超时。

本文解释这些问题并且显示什么配置技术可以用于为了防止问题。

问题：为一条断开VPN客户端环路注定的数据包在内部网络里面

当远程访问VPN用户从ASA防火墙时断开，数据包现在内部网络(注定为那些断开用户)和指定IP VPN地址也许变得循环在内部网络内。这些信息包环路也许造成在ASA的CPU使用情况增加直到循环停止或者由于在减少的IP数据包报头的IP TTL值到0，或者用户重新连接，并且IP地址被再分配给VPN客户端。

为了了解更加好此的方案，请考虑此拓扑：



在本例中，远程访问客户端分配10.255.0.100的IP地址。在本例中的ASA连接对同一网络内部分段与路由器一起。路由器有两另外的第3层网络分段连接对它。相关接口(路由)和ASA的VPN配置和路由器在示例显示。

ASA配置优点在本例中显示：

```
interface GigabitEthernet0/0
nameif outside
security-level 0
ip address 198.51.100.100 255.255.255.0
!
interface GigabitEthernet0/1
nameif inside
security-level 100
ip address 10.1.0.1 255.255.255.0
!
```

```
same-security-traffic permit intra-interface
!
ip local pool VPNpool 10.255.0.1-10.255.0.255
!
route outside 0.0.0.0 0.0.0.0 198.51.100.1
route inside 10.0.0.0 255.0.0.0 10.1.0.2
```

路由器配置优点在本例中显示：

```
interface FastEthernet0
description connected to the inside interface of the ASA G0/1
ip address 10.1.0.2 255.255.255.0
!
interface FastEthernet1
 description connected to network segment
 ip address 10.2.0.1 255.255.255.0
!
interface FastEthernet2
 description connected to other network segment
 ip address 10.3.0.1 255.255.255.0
!
ip route 0.0.0.0 0.0.0.0 10.1.0.1
```

路由器的路由表连接对ASA的里面有一个默认路由指向10.1.0.1 ASA内部接口。

当用户通过对ASA时的VPN连接， ASA路由表显示如下：

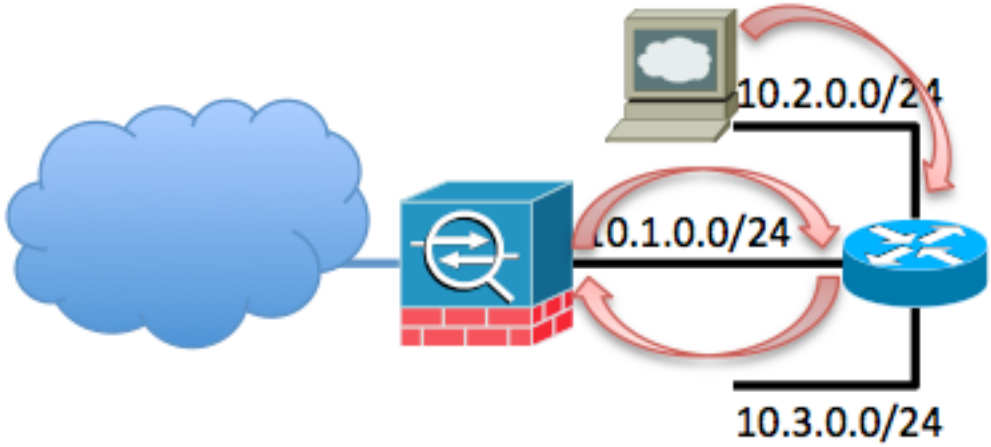
```
ASA# show route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route
Gateway of last resort is 198.51.100.1 to network 0.0.0.0
S 10.255.0.100 255.255.255.255 [1/0] via 198.51.100.1, outside
S 10.0.0.0 255.0.0.0 [1/0] via 10.1.0.2, inside
C 198.51.100.0 255.255.255.0 is directly connected, outside
C 10.1.0.0 255.255.255.0 is directly connected, inside
S* 0.0.0.0 0.0.0.0 [1/0] via 198.51.100.1, outside
```

当远程访问VPN用户从VPN，断开问题发生。这时，招待基础的路由从ASA路由表删除。如果一台主机在网络里面尝试发送流量对VPN客户端，该流量路由对ASA内部接口由路由器。步骤此系列发生：

1. 数据包被注定对10.255.0.100在ASA的内部接口到达。
2. 标准ACL检查被执行。
3. ASA路由表被检查为了确定此流量的出口接口。
4. 数据包的目的地匹配点取消内部接口往路由器的清楚的10.0.0.0/8路由。
5. ASA验证，如果发夹连接流量允许-搜索**相同的安全性permit接口内**并且发现允许。
6. 连接到/从内部接口被建立，并且数据包被退还的到路由器作为下一跳。
7. 路由器收到数据包被注定对在面对ASA的接口的10.255.0.100。路由器检查其路由表适当的下一跳。路由器发现下一跳是ASA内部接口，并且数据包发送对ASA。

8. 返回到第 1 步。

示例如下所示：



此环路出现直到此数据包减少量TTL到0。注意ASA防火墙不消耗TTL值默认情况下，当处理数据包。路由器减少TTL作为它路由数据包。这无限地防止此环路出现，但是此环路增加在ASA的数据流负载并且造成CPU使用情况阻止。

问题：VPN客户端生成的被导向的(网络)广播包在网络内部循环

此问题类似于第一问题。如果VPN客户端生成定向广播数据包对其指定IP子网(在前一个示例的10.255.0.255)，则该数据包也许转发作为单播帧由对内部路由器的ASA。内部路由器也许然后转发它回到ASA，造成数据包循环，直到TTL超时。

事件此系列发生：

1. VPN客户端计算机生成数据包被注定对网络广播地址10.255.0.255，并且数据包到达在ASA。
2. ASA对待此数据包作为单播帧(由于路由表)并且转发它到内部路由器。
3. 内部路由器，也对待数据包作为单播帧，减少数据包的TTL并且转发它回到ASA。
4. 直到数据包的TTL的进程重复减少到0。

对问题的解决方案

有几个潜在解决方案对此问题。根据网络拓扑和特殊的例子，一解决方案比别的也许是容易实现。

Null0接口的(ASA版本9.2.1和以上)解决方案1静态路由

当您发送流量对Null0接口时，导致被注定的数据包将丢弃的指定的网络。此功能是有用的，当您配置远程被触发的黑洞(RTBH)时边界网关协议(BGP)的。 在这种情况下，如果配置路由对远程访问客户端子网的Null0，它强制ASA降低流量被注定对在该子网的主机，如果具体的路由(提供由反向路由注入)不存在。

```
route Null0 10.255.0.0 255.255.255.0
```

解决方案2 -请使用不同的IP池VPN客户端

此解决方案是分配远程VPN用户与任何内部网络子网不交迭的IP地址。如果VPN用户未连接，这会将防止ASA转发数据包被注定对该VPN子网回到内部路由器。

解决方案3 -使ASA路由表特定为内部路由

此解决方案将保证ASA的路由表没有与VPN IP池交迭的任何非常清楚的路由。对于此特定网络示例，请从ASA删除10.0.0.0/8路由并且配置驻留内部接口的子网的更加特定的静态路由。从属在子网和网络拓扑编号，这也许是很大数量的静态路由，并且也许不是可能的。

解决方案4 -添加VPN子网的具体的路由取消外部接口

其他在本文描述的此解决方案是更加复杂的。思科建议您尝试首先使用其他解决方案由于在注意描述后在此部分的情况。此解决方案将防止ASA转发从VPN IP子网发出的IP信息包回到内部路由器;如果添加VPN子网的一具体的路由在外部接口外面，您能执行此。因为此IP子网为外部VPN用户保留，有一源IP地址的数据包从此VPN IP子网不应该到达入站在ASA内部接口。达到此的简便的方法是添加每远程访问VPN IP池的路由在与上游ISP路由器的一个下一跳IP地址的外部接口外面。

在此网络拓扑示例中，该路由如下所示: ：

```
route outside 10.255.0.0 255.255.255.0 198.51.100.1
```

除此路由之外，请添加**ip验证reverse-path里面**命令为了造成ASA丢弃所有数据包接收入站在从VPN IP子网来源的内部接口由于在外部接口存在的更多首选路由：

```
ip verify reverse-path inside
```

在这些命令implemeted后， ASA路由表看起来类似于此，当用户连接时：

```
ASA# show route

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route

Gateway of last resort is 198.51.100.1 to network 0.0.0.0

S 10.255.0.100 255.255.255.255 [1/0] via 198.51.100.1, outside
S 10.0.0.0 255.0.0.0 [1/0] via 10.1.0.2, inside
S 10.255.0.0 255.255.255.0 [1/0] via 198.51.100.1, outside
C 198.51.100.0 255.255.255.0 is directly connected, outside
C 10.1.0.0 255.255.255.0 is directly connected, inside
S* 0.0.0.0 0.0.0.0 [1/0] via 198.51.100.1, outside
```

当VPN客户端连接时，对该VPN IP地址的招待基础的路由是存在表里和更喜欢。当VPN客户端断开时，在内部接口到达被检查路由表，并且丢弃的由于**ip验证reverse-path里面**命令的流量从该客户端IP地址来源。

如果VPN客户端生成一个处理的网络广播对VPN IP子网，则该数据包转发到内部路由器，并且转发由路由器回到ASA，丢弃的归结于**ip请验证reverse-path里面**命令。

> **注意**：在此解决方案实现后，如果**intra-interface命令相同的安全性的permit**在配置里是存在，并且访问策略允许它，从VPN用户发出的流量被注定对在VPN IP池的一个IP地址没有连接的用户的也许路由取消在明文的外部接口。这是少见的情况，并且可以缓和与使用在VPN策略

内的vpn过滤器。如果**intra-interface命令相同的安全性的permit**在ASA的配置里，是存在此情况只发生。

同样，如果内部主机生成流量被注定对在VPN池的一个IP地址，并且该IP地址没有分配到远程VPN用户，该流量可能出口ASA的外部在明文的。